LARGE SYNOPTIC SURVEY TELESCOPE

DM Risk Management Process

prepared by: William O'Mullane, Tim Jenness

approved by: DM project manager
reference: Document-25323-01
issue: 01
revision: D
date: 2017-01-22
status: Draft

Abstract

This document defines the risk management process for DM within the overall LSST Risk management process. Some text in this document has been borrowed from Gaia DPAC, in particular Ron Drimmel worked on this originally.

Document History

Issue	Revision	Date	Author	Comment
D	1	22-01-2017	WOM	Creation

Draft

Contents

Draft

Draft

1 Introduction

Risk management has become a standard element in project management. In simplest terms, all ”risk management” means is anticipating problems and taking actions to avoid these problems: good practice for any complex endeavour. Formalising a risk management plan insures that risk management becomes a standard and regularised task in running a project.

1.1 Scope

This document defines the risk management process for the Data Management (DM) part of the LSST project.

1.2 Applicable Documents

LPM-20 Risk & Opportunity Management Plan

1.3 Reference Documents

[1] **[LSE-294]**, et al., J.K., 2013, *LSST DM Managemetn Charter*, LSE-294, URL https://docushare.lsstcorp.org/docushare/dsweb/Get/LSE-163

[2] **[LSE-163]**, et al., M.J., 2016, *Large Synoptic Survey Telescope Data Products Definition Document*, LSE-163, URL https://docushare.lsstcorp.org/docushare/dsweb/Get/LSE-163

[3] **[LPM-20]**, Krabbendam, V., Selvy, B., 2017, *Risk & Opportunity Management Plan*, LPM-20, URL https://docushare.lsstcorp.org/docushare/dsweb/Get/LPM-20

[4] **[Document-15077]**, Wolff, S., 2013, *Project Overview*, Document-15077, URL https://docushare.lsstcorp.org/docushare/dsweb/Get/Document-15077/Project%20Overview_10%208%2013.docx

Draft

1.4 Acronyms

The following table has been generated from the on-line Gaia acronym list:

Acronym	Description
CU	Coordination Unit (in DPAC)
DM	Data Management
DMLT	DM Leadership Team
DPAC	Data Processing and Analysis Consortium
DPACE	Data Processing and Analysis Consortium Executive
DPC	Data Processing Centre
ECSS	European Cooperation for Space Standardisation
JIRA	issue tracking product (not an acronym, but a truncation of Gojira, the Japanese name for Godzilla)
LSST	Large-aperture Synoptic Survey Telescope
OR	Observation Report
PC	(DPAC) Project Coordinator
RMT	Risk Management Team
TCAM	Technical Control/Account Manager
TCT	Technical Control Team

Draft

2 Project Summary

The goal of the Large Synoptic Survey Telescope (LSST) project is to conduct a 10-year survey of the sky that will deliver a 200 petabyte set of images and data products that will build a large-aperture, wide-field, optical imaging facility designed to address some of the most pressing questions about the structure and evolution of the universe and the objects in it. For more details see [Document-15077]

The DM (Data Management) subsystem represents the science ground segment of the LSST, responsible for the data processing of the data stream. Its objective is the production of a set of science pipelines to produce the LSST Science Products [LSE-163].

For further details of the responsibilities within DM see the Management Plan[1] [LSE-294].

Draft

[1] Update due April 2017

3 Risk management principles

Risk management process in DM:

- Derives naturally from LPM-20 just extending the process to all parts of DM.
- Should initially be simple and straight-forward: The risk management plan can evolve as needed.
- Should be independent of any tool adopted to assist in risk management.
- Should be a supporting activity to the project and not a burden: Administrative overhead should therefore be kept to a minimum.
- Should periodically reassess risks, to take into account experience, evolution of the project, changing context of project, etc.
- Should take place at the DM level first with major risks promoted to LSST level.

4 Risk definition

4.1 Domains of risk

See also the definitions section of LPM-20.

In the general context of project management, a risk is defined as a threat to project success because it has a negative impact on cost, schedule or technical performance.

As the primary products of DM are scientific in nature, any threat that could reduce or limit the scientific performance of the data processing can be considered as a risk. This includes factors that may have a negative impact on the precision of the data processing results. It is worth noting in this context that computing performance of the implemented SW systems can have an indirect impact on scientific performance, as implemented SW must be able to process a certain volume of data in a limited amount of time. Assuming that SW has been efficiently implemented, this constraint can place limits on the algorithms that can be adopted; if the computational cost of an algorithm is too large a less accurate (but faster) algorithm would be preferred. Therefore, if something might increase the computational cost of the data processing (i.e. an increase in the number of objects to be processed, or an increase in algorithmic complexity to reach a desired scientific precision, etc.), it represents a risk to the scientific performance.

4.2 Risk validity/Identification

A valid DM risk impacts one or more of the three domains: resources, schedule or performance (see previous section).

Draft

One of the first tasks of the risk management process is to consider and discuss proposed risks, determine their validity and select those risks which are to be documented (see task one in section 5).

Here are some examples of proposed risks and the outcome expected from such a discussion.

Proposed risk 1:

Real data is far more complex and quite different to the simulated data. Processing especially Alerts production is more computationally intensive and complex. Practically all missions experience this.

Expected conclusion:
Not accepted to be recorded as a risk because the proposal itself points out that real data will be more complex, so it is normal work to design, develop and plan for it.

Proposed risk 2:

Calculations made by one group indicate that the hardware for the computationally intensive tasks it needs to perform does not scale well. Delay may occur while the technical solution is investigated.

Expected conclusion:
This risk could be easily recorded with related severity and likelihood criteria. The initial actions and mitigation processes would be put into place, for example:
a) look for alternative hardware solutions (may increase cost, but could recover schedule)
b) set a firm date for the first technical assessment and call a DMLT meeting to address alternative and solutions.

The first example above is intended to illustrate a poor or bad risk proposal and the second is an example of a likely and reasonable proposal.

In general, a properly identified risk is composed of both cause and consequence, LPM-20 identifies the following list of assessment criteria:

1. **Identification :** identifying elements of risk or opportunity in the subsystem or Project.
2. **Establishing time frame :** determining the likely time at which a risk or opportunity event would come to pass.
3. **Assessing probability :** estimating the probability that an undesirable (for risks) or desirable (for opportunities) event may occur.
4. **Assessing severity :** gauging the severity of the impact that such an event would have on the status of the project if the event were to occur.
5. **Developing risk /opportunity handling options :**

- For risks: developing plans to avoid, accept, mitigate, or transfer
- For opportunities: developing plans to permit or promote

6. **Developing a management response :** consider how the project may respond if the event should occur

In addition for DM we should determine if the risk merits promotion to the project level risk register.

4.3 Risk scoring: severity and likelihood

Risk scoring is an attempt to qualitatively assess risks, and thus serves as an aid to objectively decide whether a risk merits attention, i.e. whether preemptive action should be taken to address the risk. Typically the two most important qualities of a risk that determines its seriousness is *severity* and *likelihood*.

For DM risk management, we adopt the severity and likelihood scales detailed below.

Risk severity is an evaluation of the consequences should a risk occur, and is measured using the following scale: Not exactly what happens in LSST .. we may need to look at this

Draft

Score	Severity	Consequences of occurrence
5	Catastrophic	Impact on resources, schedule and/or performance leads to the termination of the project.
4	Critical	Final data production is compromised, either by significantly degrading its final quality so that several mission requirements will not be met, and/or delaying its release by more than a year. Delay in first light is required. Major resource re-allocation or acquisition perhaps at the telescope.
3	Major	Occurrence causes a delay in the delivery of a non schedule critical component of more than one cycle, impacting the schedule of more than one part of DM over more than one cycle. Resources must be re-allocated between group or additional funds required, requiring intervention of LSST Project Manager. Final products are potentially compromised, so that one or more requirements will not be met unless new methods are developed or new resources can be found.
2	Significant	Occurrence implies the delivery of a low quality product (component/algorithm/data is sub-optimal, not up to specs, incomplete, etc.) on time, or a delay is necessary to reach spec. Re-assignment of resources are necessary, but adjustments can be made within the group. Schedule of more than one part of DM is compromised, but original schedule can be re-attained after 1 cycle (some development cycle milestones must be postponed to next cycle, but no more). Final products may be compromised, but all mission requirements are met.
1	Negligible	Occurrence implies some slight degradation in the quality of delivered product. Schedule of current cycle stressed, even compromised, but no impact on subsequent cycles.

Note: If any one of the consequences of a given severity applies, then the risk is at that specified severity level. Also note: Severity is determined according to consequences to the DM as a whole.

Risk likelihood is an estimate of how likely the risk may actually happen. Figure 1 shows the scale from LPM-20

#	Likelihood of Occurrence	Approximate Probability	Description of Probability
1	Rare	<1%	Likelihood of occurrence is not credible
2	Unlikely	1-5%	Not reasonalby expected to occur
3	Possible	5-10%	Possible but difficult to assess the chance or occurrence
4	Moderate	10-25%	Moderate chance of occurrence can be assessed
5	Likely	25-50%	Very likely that the event will occur
6	Almost Certain	50-75%	Near-certainty that the event will come to pass

FIGURE 1: Likelihood scale for risks from LPM-20.

These two scales (for severity and likelihood) define a two-dimensional space on which a given risk may be quantitatively mapped and thus assessed. A single code that describes the risk

assessment can be constructed from these two scales, for example an A1 risk is a risk with minimum likelihood and minimum severity, while an E2 risk is a risk with significant impact that will certainly happen at least once in the next development cycles.

An acceptance regime (used to decide whether to accept a risk or take action to reduce the risk) is defined in the severity-likelihood plane in the next section 4.4.

It may be useful to reduce the two measures above to a single *risk index*, for the purpose of prioritising a list of risks or monitoring risks over time. An example of a risk index is shown in figure 2, showing a rating going from ”Very Low” to ”Very High”.

Severity

Likelyhood	1	2	3	4	5
E	**Low**	**Medium**	**High**	**Very High**	**Very High**
D	**Low**	**Low**	**Medium**	**High**	**Very High**
C	**Very Low**	**Low**	**Low**	**Medium**	**High**
B	**Very Low**	**Very Low**	**Low**	**Low**	**Medium**
A	**Very Low**	**Very Low**	**Very Low**	**Very Low**	**Low**

FIGURE 2: Risk Index

Finally, it is worth mentioning that while the above scores and indices are quantitative they are still subjective measures, and thus can only serve as aids in the risk management process. There is no substitutes for good judgement based on experience.

4.4 Risk acceptance

The risk scores are used to define criteria for acceptance or an acceptance regime in the severity-likelihood plane. This acceptance regime is shown in figure 3.

Severity

Likelihood	1	2	3	4	5
E	**Accept**	**Act**	**Act**	**Act**	**Act**
D	**Accept**	**Accept**	**Act**	**Act**	**Act**
C	**Accept**	**Accept**	**Act***	**Act**	**Act**
B	**Accept**	**Accept**	**Accept**	**Act**	**Act**
A	**Accept**	**Accept**	**Accept**	**Accept**	**Act**

FIGURE 3: Acceptance regime

It should be noted that it is not required for a risk to fall in the acceptance regime for the RMT to recommend acceptance, particularly risks with a 'C' likelihood and a '3' severity criteria (see task 5 in section 5).

5 Risk/Opportunity management process

5.1 Roles and responsibilities

5.1.1 LSST members

The approach in DM is that all LSST members are free to identify risks through the DM risk management project in Jira.

5.1.2 Risk Management Team

The RMT is composed of the following: the DM Project Manager, the DM System Engineer and the DM Quality Assurance ManagerDo we have such a role? . This list can be extended to some technical experts depending on the risk nature.

The RMT shall be led by the PC and be responsible for:

- Maintaining the DM risks in the LSST Register.

- Any reissues of this document.
- Issuing a DM Risk Report after each risk management meeting.
- Completing a risk management cycle, as described in section 5, at least once per development cycle.
- Acknowledging new risks and monitoring registered risks, as specified in section 5.2.
- Recommends an assessment that the DMLT approves or modifies.

Risk management meetings are held by the risk management team (RMT) at least twice per year, and at least one month prior to regularly scheduled DMLT meetings. The risks actions may be monitored monthly during the DMLT teleconference.

5.1.3 DMLT

It is the DMLTOR TCT ? that has the authority to:

- Assess the acknowledged risk or, if any, approve the RMT risk assessment.
- Decide on actions to mitigate risks as needed, approving proposed action from the RMT or formulating new actions.

5.1.4 Local Risk Manager

Each DM group shall designate a Local Risk Manager (which could be the TCAM but need not be). This person shall be responsible for:

- Identifying and submitting in JIRA any new risks that will be reviewed by the RMT.
- Validating the recommendations of the RMT on existing risks affecting the group.
- Communicating to the RMT any action carried out to reduce identified risks, as well as their effectiveness.
- When appropriate, or on request of the RMT, indicate for risk, a technical expert in the group that the RMT may contact directly for necessary clarifications.

In short, the Local Risk Manager is the contact point for the RMT, and guarantees that there is at least one person in the group management structure to communicate and track the CU risks.

5.2 Risk management tasks

To assure that mitigating actions are completed on a timely basis, risk management will take place on a cyclic basis.

Figure below defines the tasks and responsible that take place over a risk management cycle. These tasks are based on the ECSS standards (ECSS-M-ST-80C) tailored to the DPAC and proposed here for LSST DM. Risk management meetings will be held on a regular basis to address these tasks, thus there is one risk management meeting per risk management cycle.

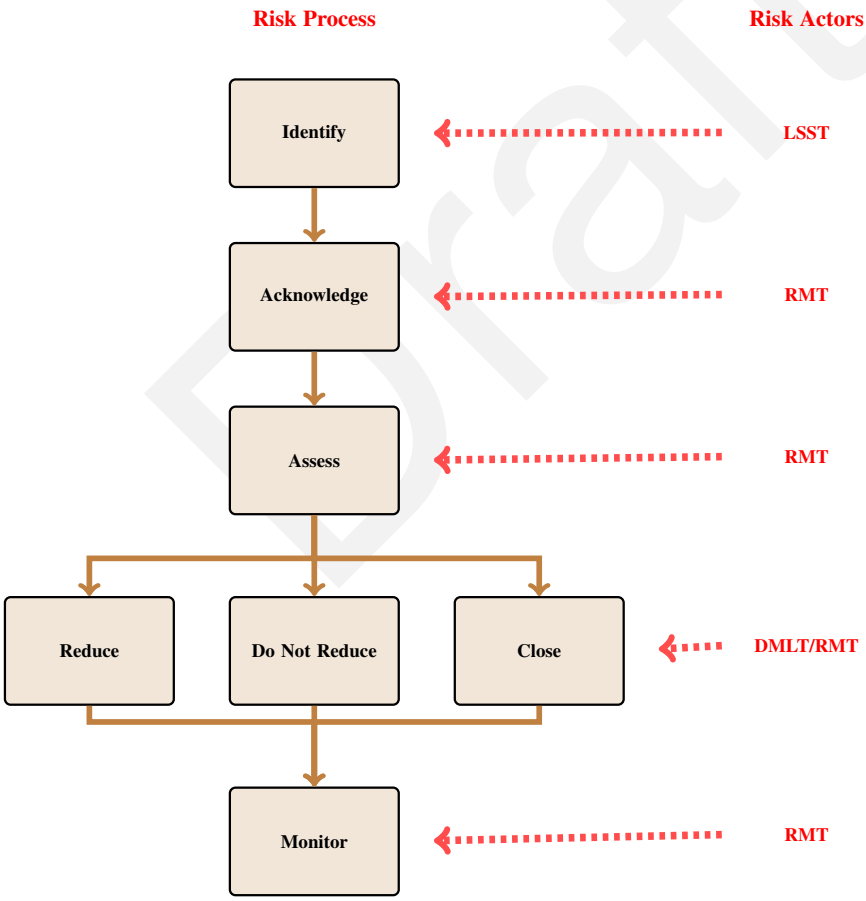

FIGURE 4: Risk Management Process

Task 1: Identify risk scenarios

It is expected that potential risks will be submitted by various parties in LSST, and indeed input of possible risks should be communicated by the CUs and DPCs.

Task 2: Acknowledge the risks

Any new risks should be reviewed by the risk management team during the risk management meeting to determine their validity. If a new risk is not considered valid, it is closed. The closed risks will be presented to DMLT. In addition, more general risk scenarios should be contemplated during the risk management meeting to identify any new risks.

Task 3: Assess the risks

For each valid risk, and for all previously identified risks, (re)assess their likelihood and severity, using the scales defined in section 4.3. The RMT recommends an assessment that the DMLT approves or modifies.

Task 4: Reduce the risks

For those risks that are deemed as ”unacceptable”, the risk management team will try to define possible actions to reduce risks in terms of occurrence and/or likelihood. The risk management team needs to balance increasing expenditure to tackle a risk.

All risks ranked as ”unacceptable” should have at least one dedicated action. The RMT should recommend mitigating actions if possible; the DMLT decides on the final actions to be taken, approving the recommendations of the RMT or formulating new actions.

Task 5: Do not reduce the risks (acceptance)

Whether or not mitigation actions are identified, there should come a time in the project when a risk can not be reduced any further. In this case the risk management team should recommend to *accept* the risk, even if it does not pass the acceptance criteria defined under task 3.

Risks should also be accepted if the cost to mitigate is greater than the cost of the consequences, obviously. More generally a risk might be accepted if the severity/likelihood of the consequences does not merit the cost to mitigate.

All accepted risks should be re-assessed at the next risk management cycle.

A risk may be closed if it is deemed unnecessary to continue monitoring the risk. This might be because it no longer applies to the project (is no longer a valid risk), or is no longer a significant risk (likelihood is null or no negative consequences). The risk management meeting may identify risks to be recommended for closing.

Task 6: Monitor the risks

After approval, the RMT is in charge of updating and issuing a new version of the Risk register. Feedback from the concerned parties is also necessary so that the risk management team can properly monitor risks. Were recommended actions taken? What were the results? Were risks

recommended for acceptance approved or not?

5.3 Risk management technical implementation

JIRA has been chosen as our Risk Management Tool in DM, this section describes the technical part of a risk registration and monitoring.

5.3.1 Use of JIRA as a risk management tool

Tim – this is a section for you to update

Jira is an issue tracking tool that has been adopted by LSST to assist and coordinate a software development effort distributed throughout Europe. This section describes how Jira will be used as a risk management tool.

In particular, for a risk reported as a JIRA issue:

- The automatically generated JIRA issue number will be used as a unique alphanumeric risk identifier.
- The JIRA Summary serves as the short descriptive title of the risk.
- The JIRA Description serves as the full description of the risk.
- Under the JIRA Risk Register project, additional customised fields to enter the risk likelihood, severity. Changes to these fields are automatically logged by JIRA.
- Recommendations by the RMT are reported in the custom fields ”Recommendations” and ”Actions”.

5.3.2 Risk submission in JIRA

When submitting a new risk in JIRA a set of fields are to be fulfilled, some are optional. THIS NEEDS REVIEW The table below present these fields:

JIRA field	Description
Summary	Summary of the risk
Description	Complete description: • Detail of the risk. • Cause. • Possible action.
Consequence	Description of the consequences in terms of time, resource, performance.

Risk severity (optional)	See 4.3.
Risk likelihood (optional)	See 4.3.

Note that any new risk with a vague description will be **closed** by the RMT. After review by the RMT, each registered risk shall have at the following fixed properties :

- A unique alphanumerical identifier that, once assigned, will not change. It is solely the task of the RMT to assign this identifier.
- A short descriptive title.
- A full description (including both cause and proposed solution).
- Consequence of the risk in terms of time, resource, performance.
- The name of the original submitter.
- The date of submission.
- Estimated date of occurrence

In addition, each registered risk shall have the following transient properties (i.e. properties that change with time) also assigned by the RMT:

- A severity and likelihood rating, and the derived the risk index.
- The date of assessment (first assessment coincides with the date of risk registration).
- Recommended response at time of assessment (reduction or acceptance).
- JIRA status: assigned, resolved or closed.
- Actions taken (if any), when and by whom.
- ...

The submitter may provide an initial risk rating; in this case these ratings must be re-evaluated by the RMT at time of registration.

The risk identifier may contain information of the source of submission (for example, a CU number), but **not** the risk assessment scores, as these will change with time.

The list of registered risks at the DPACE level constitutes the DPAC Risk Register. The DPAC Risk Register shall be reissued after each risk management meeting.

Draft

5.3.3 Risk Process Vs JIRA Status

The figure below presents the different JIRA status through the Risk Process, the blue boxes are the JIRA status:

FIGURE 5: JIRA Status through Risk Process

Note that all 'unacceptable' risk with an 'assigned' JIRA Status have at least one dedicated action monitored in JIRA.

5.3.4 Risk change tracking

An identified risk has a natural "life-cycle": a beginning, a middle and an end. These three parts correspond to risk registration, a monitoring phase and eventual risk closing. All risks surviving to the end of project are of course retired at project's end. During its lifespan a risk is constantly monitored and reassessed, perhaps acted on and (perhaps) reduced. In short, a risk accumulates a history.

The history of a risk is essentially a history of all past values of its transient properties. Tracking the history of risks is an important part of risk monitoring.

In addition to the Risk Register, the RMT shall issue a Risk Report from JIRA after each risk management meeting, with summary statistics of the current risks and overall risk trends.

Draft